Lecture 5: Algebra

Algebra is the theory of **algebraic structures** like "groups" and "rings". The theory allows to solve polynomial equations, characterize objects by its symmetries and is the heart and soul of many puzzles.
Lagrange claims that **Diophantus** is the inventor of Algebra, others think that the subject started with solutions of **quadratic equation** by **Mohammed ben Musa Al-Khwarizmi** in the book Al-jabr w'al muqabala of 830 AD. Solutions to equation like $x^2 + 10x = 39$ are solved there by **completing the squares**: by adding 25 on both sides of the equation, one obtains $x^2+10x+25 = 64$ and so $(x + 5) = 8$ so that $x = 3$.
The use of **variables**, which is a characteristic of what we now call **elementary algebra**, were introduced later. Ancient texts dealt with particular examples and calculations were done with concrete numbers in the realm of **arithmetics**. It was **Francois Viete** (1540-1603), who had the fundamental idea of using letters A, B, C, X for variables. A great moment in mathematics.

The search for formulas for polynomial equations of degree 3 and 4 lasted 700 years. In the 16'th century finally, the cubic equation and quartic equations were solved. **Lodovico Ferrari** shows that the quartic equation can be reduced to the cubic. **Niccolo Tartaglia** and **Gerolamo Cardano** showed how to reduce the cubic to the quadratic: [first remove the quadratic part with $X = x-a/3$ so that X^3+aX^2+bX+c becomes the **depressed cubic** x^3+px+q. Now substitute $x = u - p/(3u)$ to get a quadratic equation $(u^6 + qu^3 - p^3/27)/u^3 = 0$ for u^3.]
For **quintic equations**, no formulas could be found. It was **Paolo Ruffini**, **Niels Abel** and **Évariste Galois** who realized that there are no formulas in terms of roots which allow to "solve" equations $p(x) = 0$ for polynomials p of degree larger than 4. An amazing achievement and the birth of a central part of modern algebra: "group theory".

Two important algebraic structures are **groups** and **rings**.

In a **group** G one has an operation $*$, an inverse a^{-1} and a one-element 1 such that $a * (b * c) = (a * b) * c, a * 1 = 1 * a = a, a * a^{-1} = a^{-1} * a = 1$. For example, the nonzero fractions p/q with multiplication operation $*$ and inverse $1/a$ form a group. The integers with addition and inverse $a^{-1} = -a$ and "1"-element 0 form a group too. A **ring** has two compositions $+$ and $*$, where the plus operation forms an group satisfying $a + b = b + a$ in which the one element is called 0 and where the $*$ operation on nonzero elements has all group properties except the existence of an inverse. The two operations are glued together by the **distributive law** $a * (b + c) = a * b + a * c$.
An example of a ring are the **integers** or the **rational numbers** or the **real numbers**. The later two are actually **fields**, rings for which the multiplication is a group too. The integers are no field because an integer like 5 has no multiplicative inverse.

Why is the theory of groups and rings not part of arithmetic? First of all, a crucial ingredient of algebra is the appearance of **variables** and computations with these algebras without using concrete numbers. Second, the algebraic structures are not restricted to "numbers". Groups and rings are general structures and extend for example to objects like the set of all possible symmetries of a geometric object. The set of all **similarity operations** on the plane for example form a group.
An important example of a ring is the **polynomial ring** of all polynomials. Given any ring R and a variable x, the set $R[x]$ consists of all polynomials with coefficients in R. The addition and multiplication is done like in $(x^2 + 3x + 1) + (x - 7) = x^2 + 4x - 7$. The problem to factor a given polynomial with integer coefficients into polynomials of smaller degree: $x^2 - x + 2$ for example can be written as $(x + 1)(x - 2)$ have a number theoretical flavor. Because symmetries of some structure form a group, we also have intimate connections with geometry. But this is not the only connection. Geometry also enters through the polynomial rings with several variables. Solutions to $f(x, y) = 0$ leads to geometric objects with shape and symmetry which sometimes even have their own algebraic structure. They are called **varieties**, a central object of **algebraic geometry**.

Arithmetic introduces addition and multiplication of numbers. Both form a group. The operations can be written additively or multiplicatively. Lets look at this a bit closer:
For integers, fractions and reals and the addition $+$, the 1 element 0 and inverse $-g$, we have a group. Many groups are written multiplicatively where the 1 element is 1. In the case of fractions or reals, 0 is not part of the multiplicative group because it is not possible to divide by 0. The nonzero fractions or the nonzero reals form a group. In all these examples the groups satisfy the commutative law $g * h = h * g$.
Here is a group which is not commutative: let G be the set of all rotations in space, which leave the unit cube invariant. There are 3*3=9 rotations around each major coordinate axes, then 6 rotations around axes connecting midpoints of opposite edges, then 2*4 rotations around diagonals. Together with the identity rotation e, these are 24 rotations. The group operation is the composition of these transformations.
An other example of a group is S_4, the set of all permutations of four numbers $(1, 2, 3, 4)$. If $g : (1, 2, 3, 4) \to (2, 3, 4, 1)$ is a permutation and $h : (1, 2, 3, 4) \to (3, 1, 2, 4)$ is an other permutation, then we can combine the two and define $h * g$ as the permutation which does first g and then h. We end up with the permutation $(1, 2, 3, 4) \to (1, 2, 4, 3)$.
The rotational symmetry group of the cube happens to be the same than the group S_4. To see this "isomorphism", label the 4 space diagonals in the cube by $1, 2, 3, 4$. Given a rotation, we can look at the induced permutation of the diagonals and every rotation corresponds to exactly one permutation.

The rotational symmetry group as well as the full rotation-reflection symmetry group can be introduced for any geometric object. For shapes like triangles, cubes, octahedrons or polyhedra for tilings in the plane.

Symmetry groups of an object allows algebra to describe geometric shapes.

Many puzzles are groups. For a long time, the most popular puzzle was the **15-puzzle**. It was invented in 1874 by **Noyes Palmer Chapman** in the state of New York. If the hole is given the number 0, then the task of the puzzle is to order a given random start permutation of the 16 pieces. To do so, the user is allowed to transposes 0 with a neighboring piece. Since every step changes the signature s of the permutation and changes the taxi-metric distance d of 0 to the end position by 1, only situations with even $s + d$ can be reached. It was **Sam Loyd** who suggested to start with an impossible solution and offer 1000 dollars for a solution. The **Rubik cube** is an other famous puzzle, which is a group too. Exactly 100 years after the invention of the 15 puzzle, the Rubik puzzle was introduced in 1974.

Many puzzles are groups.

Probably the simplest example of a Rubik type puzzle is the **pyramorphix**. It is a puzzle based on the tetrahedron. Its group has only 24 elements. It is the group of all possible permutations of the 4 elements. It is the same group as the group of all reflection and rotation symmetries of the cube in three dimensions and also is relevant when understanding the solutions to the quartic equation discussed at the beginning. The circle is closed.